IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA	)	
	)	
Plaintiff,	)	Civil Action No. 15-1315
	)	
v.	)	
	)	
ANDREY GHINKUL	)	
a/k/a Andrei Ghincul	)	
a/k/a "smilex,"	)	
	)	
MAKSIM VIKTOROVICH YAKUBETS	)	
a/k/a "aqua," and,	)	
	)	
IGOR TURASHEV	)	
a/k/a "nintutu,"	)	
	)	
Defendants.	)	

ORDER IMPOSING PERMANENT INJUNCTION

This Order arises from a civil action filed by the Plaintiff, the United States of America, wherein the United States filed a complaint for injunctive relief pursuant to 18 U.S.C. §§ 1345 and 2521, based on Defendants' violations of 18 U.S.C. §§ 1343, 1344, and 2511. The United States moved for a temporary restraining order and an order to show cause why a preliminary injunction should not be granted pursuant to Rule 65(b) of the Federal Rules of Civil Procedures and 18 U.S.C. §§ 1345(a)(1) and 2521. The United States sought injunctive relief commanding the Defendants to stop using malicious software or code in furtherance of any scheme to commit wire fraud, bank fraud, or to engage in unauthorized interception of electronic communications, and in particular, from running, controlling, or communicating with software known as Dridex, also known as Bugat, and as Cridex (collectively hereinafter "Dridex"). The United States also sought authority to conduct technical procedures to free infected computers from the control of the Defendants as well as mitigate the effects of the infections.

On October 9, 2015, this District Court granted the Government's application for a temporary restraining order and order to show cause why a preliminary injunction should not be granted against the Defendants. (Doc. 7). On October 19, 2015, this District Court granted the Government's application for a preliminary injunction against the Defendants. (Doc. 15). On December 22, 2015, this District Court entered a Modified Preliminary Injunction against the Defendants. (Doc. 19).

The Government seeks a permanent injunction in this matter as to Defendants Andrey Ghinkul, Maksim Viktorovich Yakubets, and Igor Turashev to permanently restrain and enjoin them from using malicious software or code in furtherance of any scheme to commit wire fraud, bank fraud, or to engage in unauthorized interception of electronic communications, and in particular, are prohibited from running, controlling, or communicating with software known as Dridex, on any computers not owned by the Defendants.

FINDINGS OF FACT AND CONCLUSIONS OF LAW

The Court has considered the Government's Motion for Preliminary Injunction, Motion to Modify the Preliminary Injunction, and Motion for Permanent Injunction and hereby makes the following findings of fact and conclusions of law:

1. The statutory scheme underlying this civil action specifically provides that the Court "may at any time before final determination, enter … a restraining order or prohibition, or take such other action, as is warranted to prevent a continuing and substantial injury to the United States or to any person or class of persons for whose protection the action is brought." 18 U.S.C. §§ 2521, 1345(b).

2. This Court has jurisdiction over the subject matter of this case and there is good cause to believe that it will have jurisdiction over all parties hereto; the Complaint states a claim upon which relief may be granted against the Defendants under 18 U.S.C. §§ 1345 and 2511.

3. There is good cause to believe that the Defendants have engaged in and are likely to engage in acts or practices that violate 18 U.S.C. §§ 1343, 1344, and 2511, and that the Government is, therefore, likely to prevail on the merits of this action.

4. There is good cause to believe that, unless the Defendants are permanently restrained and enjoined by Order of this Court, irreparable harm will result from the Defendants' ongoing violations of 18 U.S.C. §§ 1343, 1344, and 2511. The evidence set forth in the Government's Memorandum of Law in Support of Motion for Temporary Restraining Order and Order to Show Cause ("Memorandum of Law") (Doc. 3) demonstrate that the Government is likely to prevail on its claim that Defendants have engaged in violations of 18 U.S.C. §§ 1343, 1344, and 2511 by:

a. intentionally infecting thousands of computers with malicious software ("malware") to steal banking and other online credentials from infected computers and enlist those computers into the Dridex "botnet" (a network of other infected computers controlled by the Defendants);

b. using the Dridex malware to intercept victims' communications without authorization; and

c. using credentials stolen by the Dridex malware to access victim bank accounts and fraudulently transfer funds.

5. There is good cause to believe that if such conduct were allowed to continue, it will cause irreparable harm to both individuals and businesses in the United States. There is also good cause to believe that the Defendants will continue to engage in such unlawful actions if not permanently restrained from doing so by Order of this Court.

6. Based on the evidence cited in the Government's Memorandum of Points and Authorities in support of its motion seeking a permanent injunction, the Government is likely to be able to prove that the Defendants are engaged in activities that violate United States law and harm members of the public, and that the Defendants have continued their unlawful conduct despite the clear injury to members of the public.

7. The Government has demonstrated good cause to believe that Defendants have directed their illegal activity at individuals and businesses located in the Western District of Pennsylvania by, among other things, infecting numerous computers in this District with Dridex and by using credentials stolen by the Dridex malware to gain unauthorized access to the bank accounts of victims in this District.

8. The Government has demonstrated good cause to believe that to halt the injury caused by the Defendants, the Defendants must be prohibited from infecting computers with Dridex and from communicating with existing computers infected with Dridex.

INJUNCTIVE RELIEF

IT IS THEREFORE ORDERED that the Defendants, their representatives, and persons who are in active concert or participation with them are permanently restrained and enjoined from using malicious software or code in furtherance of any scheme to commit wire fraud, bank fraud, or to engage in unauthorized interception of electronic communications, and in particular,

are prohibited from running, controlling, or communicating with software known as Dridex, on any computers not owned by the Defendants.

IT IS FURTHER ORDERED that this Order shall be published on the websites of the Department of Justice and the Federal Bureau of Investigation.

Entered this 7th day of January, 2020.

s\Cathy Bissoon
HON. CATHY BISSOON
UNITED STATES DISTRICT JUDGE